ELECTRONIC CRIMES TASK FORCES

The United States Secret Service is committed to safeguarding the nation's critical infrastructure and financial payment systems from cyber criminals. In 2001, the USA PATRIOT Act mandated the Secret Service establish a national network of Electronic Crimes Task Forces (ECTFs) to prevent, detect, and investigate various forms of electronic crimes including cyber crime. Today, the Secret Service operates 39 ECTFs, including two based overseas in London, England, and Rome, Italy, as part of this expanding network.

The ECTF model relies on trusted partnerships between the law enforcement community, the private sector, and members of academia to combat cyber crime through information sharing, coordinated investigations, technical expertise, and training. These ECTFs are a strategic alliance of over 4,000 private sector partners; over 2,500 international, federal, state and local law enforcement partners; and over 350 academic partners. Since inception, the ECTFs have prevented over $13 billion in potential losses to victims and arrested approximately 10,000 individuals. The ECTFs are models for 21st century law enforcement, incorporating partnerships and information sharing to focus on the challenges in combating cyber crime.

www.secretservice.gov

Questions related to information in this brochure should be directed to your local U.S. Secret Service Electronic Crimes Task Force.

ELECTRONIC CRIMES TASK FORCE LOCATIONS:

ATLANTA, GA	404-331-6111
BALTIMORE, MD	443-263-1000
BIRMINGHAM, AL	205-989-5370
BOSTON, MA	617-565-5640
BUFFALO, NY	716-551-4401
CHARLOTTE, NC	704-442-8370
CHICAGO, IL	312-353-5431
CINCINNATI, OH	513-684-3585
CLEVELAND, OH	216-750-2058
COLUMBIA, SC	803-772-4015
DALLAS, TX	972-868-3200
DENVER, CO	303-850-2700
DETROIT, MI	313-226-6400
HONOLULU, HI	808-541-1912
HOUSTON, TX	713-868-2299
KANSAS CITY, MO	816-460-0600
LAS VEGAS, NV	702-868-3000
LOS ANGELES, CA	213-533-4400
LOUISVILLE, KY	502-582-5171
MEMPHIS, TN	901-544-0333
MIAMI, FL	305-863-5000
MINNEAPOLIS, MN	612-348-1800
NASHVILLE, TN	615-736-5841
NEWARK, NJ	973-971-3100
NEW ORLEANS, LA	504-841-3260
NEW YORK, NY	718-840-1220
OKLAHOMA CITY, OK	405-272-0630
ORLANDO, FL	407-648-6333
PHILADELPHIA, PA	215-861-3300
PHOENIX, AZ	602-640-5580
PITTSBURGH, PA	412-281-7825
SAN ANTONIO, TX	210-308-6220
SAN FRANCISCO, CA	415-576-1210
SEATTLE, WA	206-553-1922
ST. LOUIS, MO	314-539-2238
TAMPA, FL	813-228-2636
WASHINGTON, DC	202-406-8000
LONDON	442-07-894-0846
ROME	390-64-674-2730

Cyber Crime Investigations

U.S. Department of Homeland Security

United States Secret Service

The Criminal Investigative Division (CID) is part of the Office of Investigations at U.S. Secret Service Headquarters in Washington, DC. CID is dedicated to ensuring the U.S. Secret Service possesses the necessary and proper tools to combat cyber crime. The principle goal of CID is for each and every action taken by Secret Service personnel to be for the purpose of protecting the American people, its leaders, and its infrastructure.

CYBER INTELLIGENCE SECTION

The Cyber Intelligence Section (CIS) is a Headquarters component responsible for pursuing high-value, transnational cyber crime targets. It is also responsible for the coordination of USSS investigations involving network intrusions, data breaches, and credit card fraud via the Internet. CIS consists of both agents and analysts engaged in collecting and analyzing data from seized evidence, criminal internet sites, and confidential sources. CIS supplements the investigative efforts of the controlling USSS office by providing further analysis of seized media in a broad, agency-wide context. CIS maintains active liaison with domestic and foreign law enforcement and intelligence agencies regarding ongoing operations.

ELECTRONIC CRIMES SECTION

The Electronic Crimes Section (ECS) is responsible for providing over 400 Secret Service special agents and 2,500 state and local law enforcement officials with equipment and training in cyber-related missions. The ECS helps develop technologies, practices, and tactics for securing cyber environments, investigating cyber crime, and performing forensics on new cyber technologies.

ELECTRONIC CRIMES SPECIAL AGENT PROGRAM

The Electronic Crimes Special Agent Program (ECSAP) was established to provide special agents with advanced skills to handle network and computer forensics related to cyber incidents. There are two specializations within the ECSAP program:

Computer Forensics (CF):

CF agents are provided with specialized techniques and equipment which allows them to conduct computer forensic examinations on electronic evidence. CF agents are familiar with retrieving evidence from computers using various operating systems, digital handheld devices such as cellphones and tablets, and other forms of electronic media.

Network Intrusion Responders (NITRO):

The Network Intrusion Responders Program (NITRO) provides special agents with specialized techniques and equipment which allow them to respond to and investigate network intrusions. NITRO trained agents are familiar with computer and network architecture as well as digital evidence handling and collection. NITRO agents are trained to investigate network intrusions ranging in size from Point-of-Sale (POS) system compromises to enterprise sized network-based intrusions. NITRO agents are skilled in the detection of organized cyber criminal tactics, techniques, and procedures that seek to destabilize our financial systems and victimize users of the internet or technological solutions.

CELL PHONE FORENSIC FACILITY

Because of the widespread use of cell phones and GPS units in modern society, many crimes involve a mobile communication device that stores digital media. The Secret Service Cell Phone Forensic Facility at the University of Tulsa recognizes digital evidence recovered from mobile communications devices as critical to the protective and criminal investigative components of the agency's mission. The Cell Phone Forensic Facility has a three-pronged mission: (i) training law enforcement personnel in embedded device forensics; (ii) developing novel hardware and software solutions for extracting and analyzing digital evidence from mobile devices; and (iii) applying the hardware and software solutions in difficult examination scenarios in support of criminal investigations conducted by the Secret Service and its partner agencies. Due to the continuing evolution in sophisticated wireless devices, the facility remains a key asset in conducting difficult examinations such as devices damaged by suspects attempting to destroy digital evidence.

NATIONAL COMPUTER FORENSICS INSTITUTE

The National Computer Forensics Institute (NCFI) is a state-of-the-art facility in Hoover, AL, providing state and local law enforcement investigators, prosecutors, and judges the training necessary to conduct computer forensic examinations, cyber crime investigations, and respond to network intrusion incidents. Graduates of NCFI join the Secret Service's network of Electronic Crimes Task Forces and frequently make vital contributions to significant Secret Service investigations of transnational cyber criminals. Since 2008, NCFI has trained over 3,800 state/local law enforcement officers, prosecutors, and judicial officials representing all 50 states and three U.S. territories.

CERT LIAISON PROGRAM

The CERT Liaison Program, in partnership with the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University, leverages non-public technology and training to meet emerging challenges to the Secret Service's investigative and protective missions. The CERT Liaison Program delivers software and system development, training curriculum design, risk assessment and mitigation for critical infrastructure, as well as technical support to complex cyber crime investigations.